3-4-3

AF/2700
#43
10f3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant and Inventor	Ho Keung, TSE.
Filing Date	07/09/98
Application Number	09/112,276
Group Art Unit	2132
Examiner	Gilberto Barron Jr.
Postal Address	P.O. Box 70492, KLN Central Post Office, Hong Kong.
H.K. Tel & FAX	(852) 8105, 1090 & (852) 8105, 1091

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231 Box AF.

Sir,

Appeal Brief (Substitute)

This is not a response to Examiner's Answer to Appeal brief. I have not yet received the Examiner's Answer.

The previous Appeal brief is prepared and submitted at a time before advisory action dated Jan 14, 2003 is received, it has to be so in order it can be filed before the deadline. And therefore, this Appeal brief(Substitute) has to be submitted to include arguments in response to Examiner's indication in P.2, section 6 that "All of the Haas disclosure is available under the statute" and Examiner's statement in section 7 that "Applicant has not addressed pending claim language to overcome the prior art of Haas".

(1) **Real party in interest**-- As I am the sole inventor and applicant, there is no other real party in interest other than me.

(2) **Related appeals and interferences**— another US patent application 08/587,448 of mine for the same invention as the present application (therefore, both applications are now under a provisional double patenting rejection) was previously under appeal and then remanded to the Examiner by the Broad and prosecution was re-opened. It will be under appeal again if the Examiner does not allow it.

Further, pls note that the claim 1 of application 08/587,448 is equivalent to the claim 1

as amended in "Substitute Amendment (submitted with Substitute Appeal Brief)".

(3) Status of Claims :

22 claims presented. Claims 1, 7, 10, 12, 14, 16, 18, 20, 21, 22 are independent.

Claims 10, 11 are withdrawn from Appeal.

Claims 2, 4-6 depends directly or indirectly on independent claim 1.

Claims 8, 9 depend directly on independent claim 7.

Claims 3, 13, 17 depend directly on independent claim 12.

Claim 15 depends directly on independent claim 14.

(4) Status of Amendments :

Amendment on claims & description & title, submitted with "Formal Response to Final Office Action" filed on Dept 26 2002---not entered. Drawing showing Figures 1 & 2 submitted with "Formal Response to Final Office Action" filed on Dept 26 2002---- entered.

Amendment entitled "Submission of New Claims 21 & 22" filed on Dept 26 2002—not entered.

Amendment entitled "Amendment" for amending claims 1, 4, 7, 14, filed on Dept 26 2002—not entered.

Amendment submitted with "Formal Response to Advisory Action Dated Sept 30 2002" & "Submission of New Claim 23"—not entered.

Amendment submitted with "Second Response to Advisory Action Dated Sept 30 2002"—not entered.

Amendment entitled "Amendment of Claims 18 & 22" & "Submission of New Claim 23", both filed on Jan 7, 2003—not entered.

In conclusion, all amendments on claims after final, for overcoming the new grounds of rejections basing on Haas et al. raised in Final Office action, are not entered .

(5) Summary of Invention :

The following is a concise explanation of the invention defined in the independent claims 1, 7, 12, 14, 16, 18, 20, 21 :

Claim 1 recites a method*(refer to description, P.3 second paragraph, "second embodiment of the present invention" & P.9, first paragraph of item 5)* for protecting software from unauthorised use, comprising the steps of :

determining if identity means/information *(corresponding to "EI sub-*

program", refer to description, P.5, item 2) , is existing in a processing apparatus ;

using a favourable result of the determination as a pre-condition for causing the processing apparatus to provide user access to the software desired to be protected ;

wherein :

the identity means/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of the software desired to be protected has to be responsible ;

access to the software desired to be protected is being provided without causing one such operation being performed and the identity means/information being specific to the rightful user(s) and the software desired to be protected being licensed to the rightful user(s).

Claim 7 recites a computer software product*(corresponding to "central program", refer to description, P.2, first & second paragraph)* for protecting software publicly distributed against unauthorised use ;

the software product comprising :

identity program code*(corresponding to "EI sub-program", refer to description, P.5, item 2)* for enabling electronic commerce operation(s) for which rightful user(s) of the software desired to be protected has to be responsible ;

authorising software*(corresponding to "AS sub-program", refer to description, P.5, item 3)* effectively under the control of the rightful user(s) for, when executed, providing user access to the software desired to be protected ;

wherein :

the identity program code and the authorising software are contained in the software product in such a manner that the authorising software is prevented from

being copied therefrom individually; and

the improvement resides in the protection is basing on no hardware and/or software specific to the rightful user(s) other than the identity program code and the identity program code being specific to the rightful user(s) ;

and the identity program code and the authorising software existing in a computer readable medium .

Claim 12 recites a method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information *(corresponding to "password", refer to description, P.4, item a)* from a user of a processing apparatus having an identity software/means ;

using the first information received being correct as a pre-condition for causing the processing apparatus to provide user access to the software desired to be protected *(corresponding to "password", refer to description, P.4, item b)*;

wherein:

the identity software/means*(corresponding to "EI sub-program", refer to description, P.5, item 2)* being for providing a second information*(corresponding to "encrypted identity", refer to description, P.5, item 2)* specific to rightful user(s) of the software desired to be protected, if the correct first information is being obtained from a user thereof ; and the second information being capable of being used in enabling electronic commerce operation(s) for which the rightful user(s) has to be responsible ;

access to the software desired to be protected is being provided without causing such a operation being performed.

Claim 14 recites a method*(refer to description, P.9, second paragraph of item 5)* for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means*(corresponding to "EI sub-program", refer to description, P.5, item 2)* associated with a processing apparatus;

using a favourable result of the authentication as a pre-condition for causing the processing apparatus to provide user access to the software desired to be protected ;

wherein the identity information/means existing in such a manner that the identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of the software desired to be protected has to be responsible ;

wherein access to the software desired to be protected is being provided without causing such a operation being performed and the identity information/means being specific to the rightful user(s) and the software desired to be protected being licensed to the rightful user(s).

Claim 16 recites a method for protecting software from unauthorised use , comprising the steps of :

(a) obtaining by protection software*(corresponding to "central program", refer to description, P.2, first & second paragraph)* running on a processing apparatus, say, first processing apparatus, first information*(corresponding to "password", refer to description, P.4, item b)* from the user thereof ;

(b) determining by the protection software*(corresponding to "EI sub-program" of the "central program", refer to description, P.7, item 4)*, from the processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to the first information obtained being

consistent with third information contained in the protection software ; thereafter

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of the second information ;

(d) using a favourable result of the authentication as a pre-condition for permitting use of the software desired to be protected on the second processing apparatus ;

wherein the third information being confidential information of a rightful user of the software desire to be protected and being necessary for enabling electronic transaction(s) for which the rightful user has to be responsible ; and the method is being performed without causing such a transaction take place .

Claim 18 recites a method*(refer to description, P.7, item 4)* for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising a sub-method ; the sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying the person having a valid account *(refer to description, P.7, item 4, second paragraph)*, by the remote electronic transaction system, basing on authenticated information *(corresponding to "encrypted identity", refer to description, P.7, item 4, second paragraph, line 5, the term "unencrypted identity" is a typographical error, it should be "encrypted identity", pls refer to "argument a")* related to the person, the information being obtained from the processing apparatus ;

(c) using a favourable result of the verification as a pre-condition for determining from the processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of the information related to the hardware or/and software ;

(e) using a favourable result of the authentication as a pre-condition for permitting use of the software on the second processing apparatus, with no charge ;

wherein the sub-method a cost is being charged from the account ; and thereafter, the sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from the account the cost *(refer to description, P.8 last paragraph- P.9 second paragraph)*.

Claim 20 recites a method for protecting software, publicly distributed through a communications network*(refer to description, P.3, under the heading "Detailed description of the preferred embodiments", first paragraph)*, for use by a user, from unauthorised use ; comprising a sub-method ;

wherein the sub-method a protection software*(corresponding to "central program", refer to description, P.2, first & second paragraph)* being used and "the presence of identity information/means*(corresponding to "EI sub-program" of the "central program", refer to description, P.7, item 4)* in a processing apparatus" is being used in the creation of the protection software as a pre-condition for the protection software to perform in the processing apparatus step (a) below ; and the identity information/means being specific to the user and capable of being used in enabling electronic commerce operation(s) for which the user has to be responsible ;

the sub-method comprising the steps of :

(a) determining by the protection software*(corresponding to "EI sub-program" of the "central program", refer to description, P.7, item 4)* running on a processing

apparatus, say, first processing apparatus with the precondition being met, first information related to the hardware or/and software of the first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if the second information is consistent with the first information ;

(d) using a favourable result of the determination of consistence as a pre-condition for permitting use of the software desired to be protected on the second processing apparatus ;

thereafter, the sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing **any** user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor *(refer to description, P.8 last paragraph- P.9 second paragraph)* .

Claim 21 recites a method for verifying identity of a user of a data processing apparatus, comprising the steps of :

a) receiving, by the data processing apparatus, information*(corresponding to "password", refer to description, P.4, item b)* specific to a user and necessary for accessing an account of the user ;

b) verifying the account being valid *(refer to description, P.7, item 4, second paragraph)*, by an electronic transaction system, by use of the information received by the data processing apparatus;

c) using by the data processing apparatus, a favourable result of the verification as a pre-condition for providing user access to at least a part of the functionality of the data processing apparatus ;

wherein the steps a) to c) are being performed without charging the account and the at least a part of functionality being not related to the validity status of the account.

(6) Issues :

A) Whether "unencrypted identity", in description, P.7, item 4, second paragraph, line 5, is a typographical error and should be "encrypted identity" ?

B) Whether claims 1, 9 and 22 are unpatentable under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the present invention ?

C) Whether claims 7-9 are unpatentable under 35 U.S.C. 102(b) as being anticipated by Wiedemer(4,796,181)?

D) Whether claims 1, 2, 4, 14, 15 and 17-22 are unpatentable under 35 U.S.C. 103(a) over Wiedemer(4,796,181) in view of Haas et al (5,719,938 issued Feb17, 1998, filing date Aug 1,1994)?

E) Whether claims 12, 13 and 16 are unpatentable under 35 U.S.C. 103(a) over Wiedemer(5,155,680) in view of Haas et al (5,719,938 issued Feb17, 1998, filing date Aug 1,1994)?

(7) Grouping of Claims

Regarding rejection of claims 7-9 under 35 U.S.C. 102(b) as being anticipated by Wiedemer(4,796,181), claims 7-9 belong to a group.

Regarding rejection of claims 1, 2, 4, 14, 15 and 17-22 under 35 U.S.C. 103(a) over Wiedemer(4,796,181) in view of Haas et al, claims 1, 2, 4, 14,15 belong to a first group ; claims 18,19 belong to a second group ; claim 20 belongs to a third group ; claim 21 belongs to a fourth group.

Regarding rejection of claims 12, 13 and 16 are unpatentable under 35 U.S.C. 103(a)

over Wiedemer(5,155,680) in view of Haas et al, claims 12,13 belong to a group and claim 16 belongs to another group.

The different groups do not stand or fall together.

(8) Argument

Argument A:

Whether "unencrypted identity", in description, P.7, item 4, second paragraph, line 5, is a typographical error and should be "encrypted identity" ?

As readable in the description, P.7, item 4, second paragraph, lines 4-6 that "In the initialization process, the central program sends to the central computer, as mentioned herein above in **item 2**, an **unencrypted** identity of the rightful user of the central program", the term "**unencrypted**" is a typographical error and the correct term should be "encrypted", for the reason that in P.5, **item 2** of the description, it is disclosed a "Sub-program for providing an Encrypted Identity (EI sub-program)", in which unencrypted identity or its equivalent is not being mentioned.

Argument B:

Whether claims 1, 9 and 22 are unpatentable under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the present invention ?

In support of this rejection, the Examiner states in the Final Office Action that i) "Claim 1 is indefinite for the term "means/information", ii)"means" invokes the 6th paragraph of section 35 USC 112 ii) this requires the interpretation of "means" to correspond to what is disclosed in the specification and finally, iv) that it does not allow determination of what is disclosed in the specification, eg., is it information or a software module.

I contend that the term "means" is directed to any software means or hardware means or a combination thereof meeting the all other requirements of identity means of claim 1. And in the description it does not merely mention the software aspect of the identity means, the hardware aspect is implicitly indicated in P.3, under the heading "Detailed description of the preferred embodiments", first paragraph, line 4, "a user's IBM PC computer". Further, the term "means" does not invoke the 6th paragraph of section 35 USC 112 as the phrase "means **for**" is not being used.

Still Further, although not explicitly indicated in claim 1, from its requirement "said identity means/information, if so existing, being **capable of** being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible", it should be understood therefrom that, the identity information itself as claimed or the identity means as claimed is capable of being used to generate information, which being **information can be actually used** to be authenticated, by an electronic transaction apparatus trusted by a counterpart involved in the electronic commerce or a trusted party such as a clearing house, so as

to enable electronic commerce operation(s) for which the rightful user(s) cannot deny responsibility. The identity information/means as claimed should be created by the electronic transaction apparatus in a confidential manner and be made available only to its rightful user.

Therefore, the identity information or the identity means as well as the information it generated is well defined and cannot be met by any existing information/means not being specifically made for the rightful user(s) for the purpose of enabling electronic commerce operation(s).

Finally, the term "identity means/information" is defining a structure or its equivalent well known to those in the art .

In support of this rejection, the Examiner also states in the Final Office Action that claim 1 is indefinite as "favourable" is a relative term and it is not clear to whom would apply "favourable". The Examiner further instructs to use terms that are present in the specification that correspond to this step.

I contend that Claim 1 recites "a method for protecting software from unauthorised use" in the preamble, so it should be very clear that "a favourable result" of determination of existence of identity means/information in a processing apparatus, which being used as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected, is a positive result, that is, the identity means/information is existing in the processing apparatus, otherwise the method as claimed cannot protect software from unauthorized use. Further, in response the Examiner's instruction, I have filed amendment to eliminate "favourable" and to use terms that are present in the specification that correspond to this step, but was refused entry by the Examiner as "new issue", the amendment is submitted again with this Appeal Brief.

In support of this rejection, the Examiner also further states in the Final Office Action that claim 9 is definite because they claim a "carrier wave"-not a physical thing, as such cannot be claimed. Claim 22 is indefinite because it seeks to patent a program per se-a program per se is a data structure and not a physical thing. The Examiner also states in the advisory action dated Sept 30, 2002, P.3, item 10, that claim 9 is indefinite as it is not clear how computer readable medium being in the form of a data signal embodied in a carrier wave can function to store the recited identity program code.

I contend that they are commonly used languages found published US software patent, some of them are listed as follows:

United States Patent 6,467,037

Griesemer

October 15, 2002

Claim 10. A computer program product that executes instructions, comprising:

computer code for maintaining a program counter .....

.....;

a computer readable medium that stores the computer codes.

11. The computer program product of claim 10, wherein **the computer readable medium is** selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and **data signal embodied in a carrier wave.**

United States Patent *6,349,408*

Smith **February 19, 2002**

Techniques for implementing a framework for extensible applications

Primary Examiner: Dam; Tuan Q.

Assistant Examiner: Zhen; Wei

Claims

What is claimed is:

16. A computer program product for providing a software module within an application, comprising:

computer code that receives a software module .....;

.....

a computer readable medium that stores the computer codes.

17. The computer program product of claim 16, wherein **the computer readable medium is** selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and **data signal embodied in a carrier wave.**

United States Patent *6,351,751*

Traversat , et al. **February 26, 2002**

Persistent storage managers for configuring client/server environments

Primary Examiner: Black; Thomas

Assistant Examiner: Rones; Charles L.

Claims

What is claimed is:

18. A computer program product for initializing a client subsystem, comprising:

computer code that instantiates a first persistent manager object on a client subsystem...;

....

a **computer readable medium that stores the computer codes**.

19. The computer program of claim 18, wherein t**he computer readable medium is** selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and **data signal embodied in a carrier wave**.

Argument C:

Whether claims 7-9 are unpatentable under 35 U.S.C. 102(b) as being anticipated by Wiedemer(4,796,181)?

The Examiner states in the Final Office Action, P.5, section 12, that "SECURITY MODULE 16 corresponds to the recited identity software. Column 6 lines 41-49 describes that the billing module provides information for enabling **a billing operation** to the user **take place whenever the protected software is to be executed**".

Regarding independent claim 7, it recites the "authorising software for providing user access to said software desired to be protected", is being "**effectively under the control of the rightful user thereof**", this means that the rightful user(s) can use the authorising software to access the protected software without any permission from other parties, this implies that no billing operation is necessary.

The present invention as defined by claim 7 allow unrestricted rightful use of protected software while offering protection against unauthorised use by requiring the authorising software be contained in the protection software product with the identity program code, and can not be copied therefrom individually. The identity program code being for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible.

Accordingly, Wiedemer(4,796,181) cannot meet independent claim 7 and the rejection thereof and its dependent claims 8, 9 should be withdrawn .

Wiedemer + Haas et al

I have also considered whether the present claim 7 can be met by Wiedemer if the teaching of another reference Haas et al is applied thereto, but I found that they fail to meet the present claim 7, for the following reasons :

As readable on column 5, lines 47-54, Haas et al. merely teach a deterrent as causing by a software, a rightful user's credit card number to be displayed, to discourage a rightful user from sharing the software which being for decrypting a commercial software product, to other people. This deterrent although may be useful, it has a drawback that the rightful user have to make sure no other people is around before he can use the software.

The present invention as claimed by claim 7 is directed to a method for protecting software from unauthorised use. As readable therefrom, it requires existence of the identity program code as a pre-condition for providing user access to the software desired to be protected. Thus, the invention as defined by claim 7 is useful for protecting a software from unauthorised use at a time after purchase and no further payment for the use thereof is to be made.

Although not indicated in claim 7, it is obvious that the identity program code is stored in a computer device and is not in a human visible form and not accessible to any one else except under the permission of the rightful user.

It is an essential feature in Haas et al.'s teaching that a rightful user's credit card number has to be displayed, and it is therefore not obvious to one with ordinary skill in the art to modify it by not having the credit card number to be displayed; and further to make use of the electronic commerce capability of the credit card number to

create a program to enable a computer to make electronic commerce operation(s) to meet requirement of "identity program code" of claim 7; and still further, to combine the identity program code with an authorising software which being for providing user access to the software desired to be protected, in such a manner the authorising software is prevented from being copied individually, so as to amount to the present invention as defined by claim 7.

It is respectfully submitted that "the credit card number to be displayed" of Haas et al. disclosure and "credit card number exist in a software to enable electronic commerce operation(s) such as internet transactions or the like" exist in a computer in 2 technical distinguishable forms. The reason is, the former is in human readable form and the latter is in a form agreeable with a common communication protocol for communicate to/understandable by an existing remote transaction system. Therefore, "the credit card number to be displayed" of Haas et al. cannot meet the requirement of "identity program code for enabling electronic commerce operation(s)" of claim 7 literally.

Further, Wiedemer merely disclose an identity means which being a billing module, "that leads to a billing charge, but does not disclose the step of not causing an operation for which an authorized user is responsible for", as the Examiner admitted in his office action. It is respectfully submitted that, it is impossible for one with ordinary skill in the art to modify Wiedemer's billing module which most important purpose is to charge a user for usage of software, to not charge the user so as to meet the important limitation "authorising software" of claim 7 that it has to be "effectively under the control of said rightful user(s) for". And, it would also not be obvious to one with ordinary skill in the art to apply Haas et al. to Wiedemer as the existence of billing operation is already providing a better discouraging effect-it requires actual

payment.

Argument D:

Whether claims 1, 2, 4, 14, 15 and 17-22 are unpatentable under 35 U.S.C. 103(a) over Wiedemer(4,796,181) in view of Haas et al (5,719,938 issued Feb 17 1998, filing date Aug 1,1994)?

As the Examiner has admitted in the Final Office action, P.6, section 13, second paragraph, in his arguments in support of 103 rejection of claims 1, 2, 4, 14, 15 and 17-22, "The Wiedemer patent provides for an identity means to determine authorization if a user and provides for information that leads to a billing charge, but does not disclose the step of not causing ..electronic commerce operation to be performed".

But the Examiner further stated, in the Final Office action, P.6, section 13, third paragraph, "The patent to Haas et al teaches a method for providing secure access to shared information such as a newspaper, see column 1, lines 20-35. The Haas patent teaches deterrents for discouraging users from providing useful information to others to access the information in question. Column 5, lines 47-54 teach a first deterrent as causing a rightful user's credit card number to display to discourage a rightful user from sharing the information to access the secured information to others".

Finally the Examiner concluded in the fourth paragraph, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wiedemer method as taught in Hass by causing a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others who are not the rightful user(s).

Regarding independent claims 1, 14, the Board is respectfully requested to consider the allowability of claims 1, 14 as amended in the amendment entitled "Substitute Amendment (submitted with Substitute Appeal Brief)", for overcoming this new ground of rejection basing on Haas et al. raised in Final Office Action. Pls note that no amendment request for overcoming this new ground of rejection Haas et al., is entered after final.

The Examiner's rejections are respectfully requested.

Regarding independent claims 18, 20, they are directed to a method for protecting software from unauthorized use, basing on hardware or/and software configuration/characteristics of a processing apparatus of a user, but at the same time enables the user to use the protected software on different processing apparatus with different software/hardware characteristics, without recharging the user the cost of the protected software once it has been paid. This is another innovative feature of the present invention not being suggested or disclosed by the cited prior art references Haas et al and the 2 Wiedemer patents, either considered individually or in combination.

Independent claims 18, 20 recite a step (c), (a) respectively, for **recognising** by determing information related to hardware or/and software thereof, **a processing device,** in the present of an identity information or means and **thereafter, permitting use of software desired to be protected thereon** .

Claim 18, in particular, recites a sub-method for **a favourable result of a verification of validity of a user's account** as a pre-condition for recognising a processing device(refer to step c), for a cost from that account. It is clearly understood that the cost is for the use of the protected software on that recognised processing device by that user, because thereafter no further charge therefor, as readable on step (e).

Independent claims 18 further recites, thereafter, the sub-method capable of being used for **recognising another processing device, without re-charging the cost.**

Thus, a user who has paid for the protected software, can use the same on any processing device he desires or on the original processing device after changes in software/hardware, without being fully re-charged, by the present method as defined by claim 18 which assures the software vendor that the protected software will continue to be used by that user.

Claim 20 recites "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform ... step (a)". This actually means that the protection software either determines the presence of identity information/means, like claim 1, or being combined with the identity program code in a non-separable manner, like claim 7. Further, claim 20 recites a sub-method which after **recognising a first processing device** (refer to step (a)), capable of being used for **recognising another processing device, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor.**

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claims 18, 20 and their dependent claims 17, 19 is respectfully requested.

Regarding independent claim 21, although not readable on claim 21, the present invention as defined by claim 21 is directed to a method for protecting a data processing apparatus from unauthorised use.

It is respectfully submitted that, it is an innovative feature of the present invention as defined by independent claim 21 that , verifying identity of a user of a data processing apparatus, a) by receiving information specific to a user and necessary

for accessing an account of the user; b) verifying the user account being valid; c) and using a favourable result of the verification as a pre-condition for providing user access to at least a part of the functionality of the data processing apparatus, **without charging the account and that at least a part of functionality being not related to the validity status of the account**.

Throughout Haas et al and Wiedemer, whole document, there is no disclosure or suggestion that "validity of a user account should be checked, without charging the account for providing the user access to a data processing apparatus", as required by claim 21. In Haas et al. at column 3 lines 55-60, "the user i transmits ...his credit card number (for billing purposes)", it is clear that the credit number which is for billing purposes cannot meet this important requirement of claim 12 .

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claim 21 is respectfully requested.

Argument E:

Whether claims 12, 13 and 16 are unpatentable under 35 U.S.C. 103(a) over Wiedemer(5,155,680) in view of Haas et al (5,719,938 issued Feb 17 1998, filing date Aug 1,1994)?

As the Examiner has admitted in the Final Office action, P.7 section 14, second paragraph, in his arguments in support of 103 rejection of claims 12, 13, 16 , "The Second Wiedemer patent (5,155,680) discloses a billing system similar to the first Wiedemer patent (4,796,181) and provides the same component...this patent also provides for PIN, i.e. password protection".

The Examiner further stated, in the Final Office action, P.7, section 14, third paragraph, "Haas et al teaches a method for providing secure access to shared information such as a newspaper, see column 1, lines 20-35. The Haas patent teaches deterrents for discouraging users from providing useful information to others to access the information in question. Column 5, lines 47-54 teach a first deterrent as causing a rightful user's credit card number to display to discourage a rightful user from sharing the information to access the secured information to others".

Finally the Examiner concluded in the fourth paragraph, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Wiedemer method as taught in Hass by causing a rightful user's credit card number to be displayed in order to discourage rightful user's from sharing information with others who are not the rightful user(s).

Regarding independent claim 12, the Board is respectfully requested to consider the allowability of claim 12 as amended in the amendment entitled

" Substitute Amendment (submitted with Substitute Appeal Brief)", for overcoming this new ground of rejection basing on Haas et al. raised in Final Office Action. Pls note that no amendment request for overcoming this new ground of rejection Haas et al., is entered after final.

The Examiner's rejections are respectfully requested.

Regarding independent claim 16, it recites a method in which if first information is obtained from a user in step (a), then in step (b), it will **recognise a** by determing information related to hardware or/and software thereof, **processing device,** and **thereafter, permitting use of software desired to be protected thereon** .

Further, Claim 16 recites the first information has to be consistent with third information which being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible; and the method is being performed **without causing a such transaction take place** .

In conclusion, claim 16 is directed to a method for protecting software from unauthorized use, basing on hardware or/and software configuration/characteristics of a processing apparatus of a user, but at the same time enables the user to use the protected software on different processing apparatus with different software/hardware characteristics, without recharging the user once the cost of the protected software has been paid. This is an innovative feature of the present invention not being suggested or disclosed by the cited prior art references Haas et al and the 2 Wiedemer patents, either considered individually or in combination.

Accordingly, withdrawal of the 35 USC 103 (a) rejection of independent claim 16 is respectfully requested.

Respectfully submitted,

Applicant & Sole Inventor,

Ho Keung, Tse.

(9) Appendix.

1. A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means/information, is existing in a processing apparatus ;

using a favourable result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity means/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

2. A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

determining said identity means/information as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;
and for providing user access to third software if said authentication result is favourable .

4. A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user(s).

5. A method for protecting software from unauthorised use , as claimed in claim 1, wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. A method for protecting software from unauthorised use, as claimed in claim 5, wherein said processing apparatus having an encrypted identity of its rightful user ; and if one of said protected programs stored in said processing apparatus has a valid user identity which being not consistent with the decryption result of said encrypted identity of said processing apparatus, use of said protected programs will not be permitted and will be permitted if otherwise .

7. A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected ;

wherein :

said identity program code and said authorising software are contained in said software product in such a manner that said authorising software is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user(s) other than said identity program code and said identity program code being specific to said rightful user(s) ;

and said identity program code and said authorising software existing in a computer readable medium .

8. A computer software product as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user(s) .

9. A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code and said computer readable medium being data signal embodied in a carrier wave.

10. A computer software product for protecting other software against unauthorised use , comprising :

authorising program for providing user access to said software desired to be protected ;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program as a part thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof ;

said authorising program existing in a computer readable medium .

11. A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s) and said computer readable medium being data signal embodied in a carrier wave.

12. A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed.

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14. A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a processing apparatus;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein said identity information/means existing in such a manner that said identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) and said software desired to be protected being

licensed to said rightful user(s).

15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

16. A method for protecting software from unauthorised use , comprising the steps of :

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d) using a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .

17. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

18. A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being obtained from said processing apparatus ;

(c) using a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e) using a favourable result of said authentication as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

19. A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to e) .

20. A method for protecting software, publicly distributed through a communications

network, for use by a user, from unauthorised use ; comprising a sub-method ;

wherein said sub-method a protection software being used and "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/means being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information ;

(d) using a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing **any** user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

21. A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

a) receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

b) verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

c) using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said steps a) to c) are being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

22. A software product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21 ;

said computer code existing in a computer readable medium.